The Implication on Cyber Operation in the Western Pacific and Japan-US Alliance

Col. Nomura

JAPAN AIR SELF DEFENSE FORCE

DISCLAIMER

The views, opinions, and proposals provided in this presentation are solely of the briefer's own and thus shall not be construed as official positions of either the Stimson Center or the Government of Japan.

CONTENTS

Ⅰ Introduction

Comprehensive Cyber Warfare Abilities（Richard Clarke “ *Cyber War”, 2010*）

Country	Cyber Attack	Dependence on cyber(*1)	Cyber Defense	Total (*2)
USA	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Korea	2	9	7	18

*1 The higher the reliance on the cyber domain of society is, the lower the score.
*2 The more points are stronger, the less the score is weak.

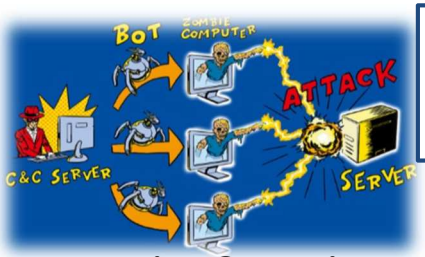
Ⅱ Positioning of cyber domain in cross-domain operation

Cross-Domain Operation seen in US military strategy

"Having a strong Air Force no longer guarantees control of the air, and having a strong Navy no longer guarantees control of the seas.
Our respective war-fighting domains have become intertwined such that the ability to control and exploit one increasingly depends on control in the others." (The American Interest, Feb 2012)

Ⅱ Positioning of cyber domain in cross-domain operation

■Case of cyber warfare（2007～2013）



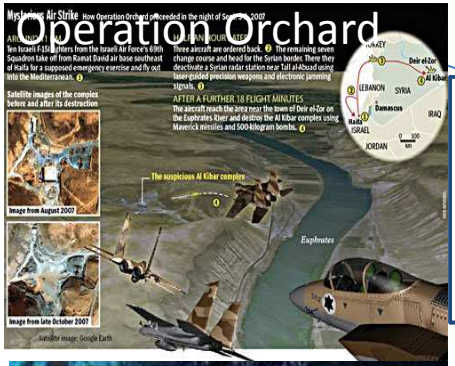
Estonia, Georgia

Estonia(2007)
Government system is down due to large DDos attack

Georgia(2008)
Large DDos attack with Russian invasion of Georgia

South Korea(2013,2014)
Banks and other systems all down due to virus infection

United States(2013)
・Sony Picture Entertainment was hacked. FBI asserts as North Korean crime
・Mandiant reported attacks by Chinese Cyber Units



Syria(2007)
During the air strikes of Israel, cyber attack against Syrian air defense network

Japan(2011)
M.H.I. computer leaked internal information due to virus infection

Iran(2010)
Nuclear fuel facilities temporarily out of control by Stuxnet

Sony Entertainment Pictures

South Korea

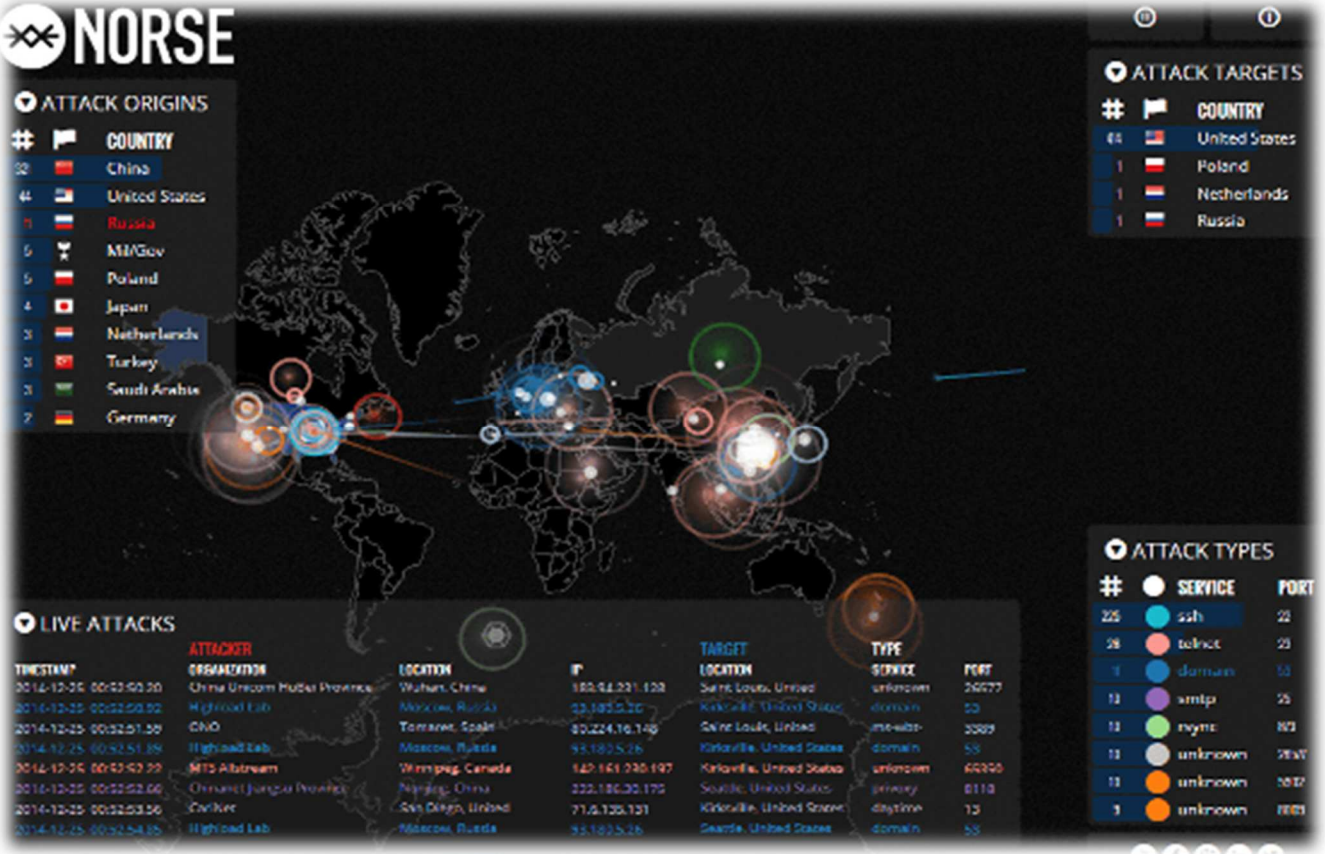
Mitsubishi Heavy Industry

Attacks by Chinese Cyber troops

Ⅱ　Positioning of cyber domain in cross-domain operation

■Case of cyber warfare（2014～）

2014　Ukrainian conflict



2016 Cyber warfare against each election in the West

Ⅱ Positioning of cyber domain in cross-domain operation

■ Similarities between Air and Cyber Domains at the beginning

Similarity	Air Domain	Cyber Domain
Connection with other Domains	Connected to land, sea, and space ⇒Operations in other domains can not be completed without the control of the air or air superiority	Domain connected across domains ⇒The superiority in the cyber domain is extremely important in carrying out integrated operations in the A2AD environment
Strategic Highlands	It became possible to obtain more information than seeing enemies from above a high hill	Cyber and the space area are “New Highlands" and in China they are referred to as “Strategic high points"
Not affected by the distance of the theater	It is possible to give a direct attack on the C.O.G of the enemy without being influenced by the front line in the land and maritime	It takes few seconds to attack intentionally anywhere in the world where you are connected via the Internet
The overwhelming advantage of the attacker	Air power with the overwhelming advantage of attack	In addition, attackers have the “Essential advantage of attack" that they can choose when, where, and how

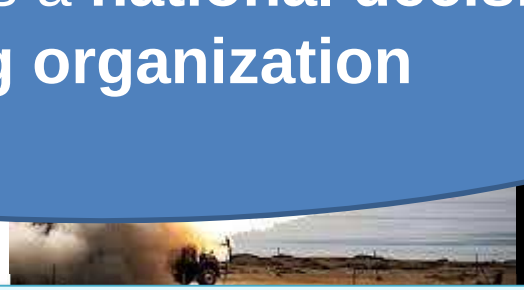
Derive implication of incorporating strategies in the Air domain that has many similarities with the cyber domain and that precedes decades

Ⅱ Positioning of cyber domain in cross-domain operation

■ Transition of Air Strategy (Strategic Air Attack)

From the situation of World War I, which was total warfare, the importance of the strategic air attack, in which cities are attacked by air power, is proposed by Giulio Douhet（*The Command of the Air*）

Giulio Douhet
（1869～1930）



【 Common point】
The main point the state's C.O.G. as a military target is a **national decision-making organization**

John A. Warden Ⅲ
（1943～）

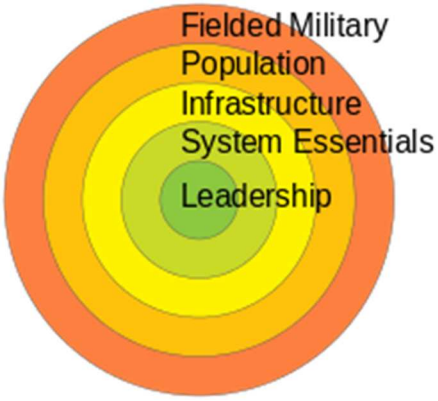
John A. Warden's air strategy is a strategy attack that causes strategic paralysis in the whole state by attacking enemy nation leaders and warfare infrastructure directly, causing the enemy's strategy to be defeated (*"The enemy as a system"*, Airpower Journal. Spring95)

Ⅱ Positioning of cyber domain in cross-domain operation

John A. Warden Ⅲ
（1943～）

Based on the "Center of Gravity (C.O.G) " advocated by Clausewitz, C.O.G of the modern state was analyzed with the hint and it was conceptualized with the "Five-Ring Model" consisting of the following five C.O.G

Center of Gravity	Link to cyber domain	Case
Leadership	State agencies such as Executive Office of the President, which are responsible for the staff function of national leaders, are subject to attack	Estonia(2007) Georgia(2008) Ukraine(2014)
System Essentials	Information on cutting edge technology relating to military technology itself is subject to attack	Cyber attack by 61398 unit (China) (2006-2013)
Infrastructure	Infrastructure for which IOT(Internet od Things) is going to be vulnerable to attack	Stuxnet(2010)
Population	Manipulate the will of the people of the opponent country with fake news	Ukraine(2014) Elections in West(2016-2017)
Fielded Military	Winning cyber superiority with Cyber weapons, advance overall operations to absolute advantage	Operation Orchard(2007)

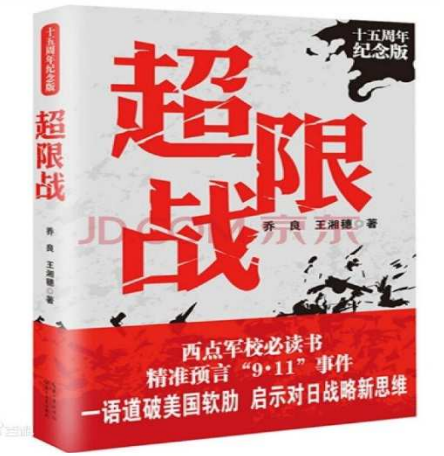


Five-Ring Model

Cyber attacks against 5 C.O.G (National Decision Making Organization) are “Strategic Cyber Attack“
Cyber attacks against an Field Military can be said to be a “Tactical Cyber Attack"

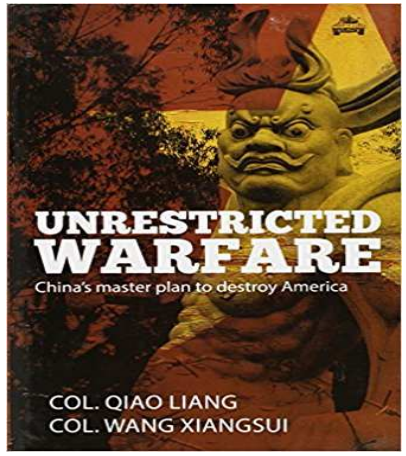
Ⅲ Cyber domain seen in China's strategy

超限战 (Unrestricted Warfare)



乔良
Col. Qiao Liang

王湘穗
Col. Wang Xiangsui



In terms of beyond-limits warfare, there is no longer any distinction between what is or is not the battlefield. Spaces is nature including the ground, the seas, the air, and the outer space are battlefield, but social spaces such as the military, politics, economics, culture, and the psyche are also battlefields. And ***the technological space liking these two great spaces*** is even more so the battlefield over which all antagonists spare no effort in contending.*(“Unrestricted Warfare”,*pp177)

Ⅲ Cyber domain seen in China's strategy

863 Program and **Assassin's Mace**

863 Program

Initiated in March 1986, China's National High-Technology Program was a major effort by China to overcome shortcomings in its national security through the use of science and technology.(The Hundred-Year Marathon)

***"Assassin's Mace** is a key component to China's military strategy in the Hundred-Year Marathon."*

(Michael Pillsbury, *The Hundred-Year Marathon*, Henry Holt, New York, 2015, pp139)

In March 1986 (during the 863 program) the **Reagan administration assisted China's development of eight national research centers** focused on genetic engineering, intelligent robotics, artificial intelligence, automation, biotechnology, lasers, supercomputers, space technology, and manned spaceflight.（Ibid., p.78.）

Ⅲ Cyber domain seen in China's strategy

What is 杀手锏 (**Assassin's Mace**)?

What is 杀手锏 (Assassin's Mace)?

Western Style

Asymmetric warfare　Attack opponent's weak point

Chinese Style

Assassin's Mace　Change opponent's strength to weak point

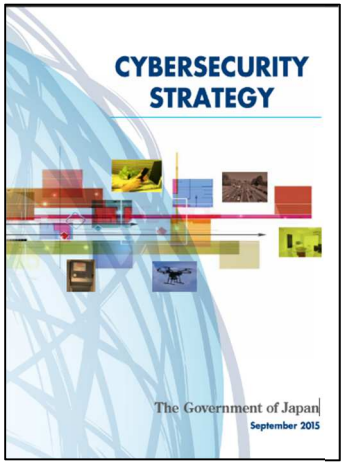
Combine Western technology with Eastern wisdom

Strong Point (U.S.)	Means of attack
Network	Cyber Attack
Global Basing Logistic Structure	Cyber Attack, ASBM
Democratic	Cyber Propaganda（Fake News）

*"Assassin's Mace concept is consistent with the long-standing Chinese military thinking … and is centered on **information warfare** and **extended-range strikes**."*

(Andrew Krepinevich, *7 DEADLY SCENARIOS*, Bantam Book, New York, 2010, pp187)

Ⅳ Approach to Cyber Domain in Japan



Cybersecurity Strategy (September 2015)
National center of **I**ncident Readiness and **S**trategy for **C**ybersecurity(**NISC**)
*"There was a potential shortage of **further 80,000** information security experts approximately in Japan."*

"The Ministers called for deepening consultations in a timely manner on Alliance responses to serious cyber incidents." (JOINT STATEMENT OF THE SECURITY CONSULTATIVE COMMITTEE, Aug 2017)

Ⅳ Approach to Cyber Domain in Japan

Japan's challenge to withstand cyber warfare

Citizen's awareness of cyber threats

No organization dealing with cyber intelligence

U.S. National Security Agency

U.K. Government Communications Headquarter

Japan?

Ⅳ Approach to Cyber Domain in Japan

Cyber attack weapon as protection reserve capacity

Phase	Indicators
Reconnaissance	Research, identification and selection of targets, often represented as crawling Internet websites

"Penalty on electromagnetic records by illegal command"
and
"Control Law of Injustice Access"

These are restricted by these two domestic laws

Reference : *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lockheed Martin

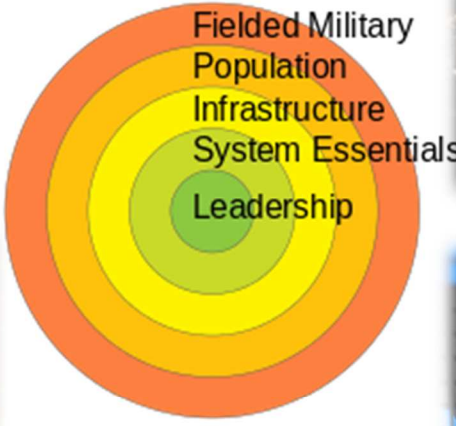
Ⅳ Approach to Cyber Domain in Japan

Cyber abilities necessary for Japan

The organization responsible for cyber intelligence

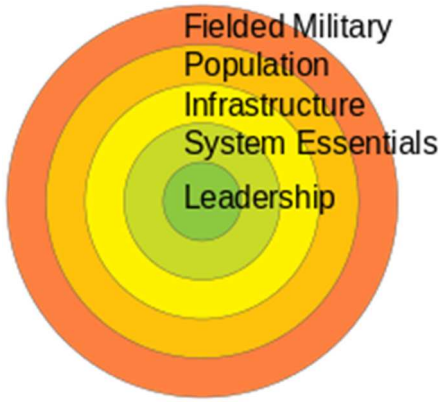
Cyber attack weapon as protection reserve capacity

Clarify the strategic goal of cyber attack



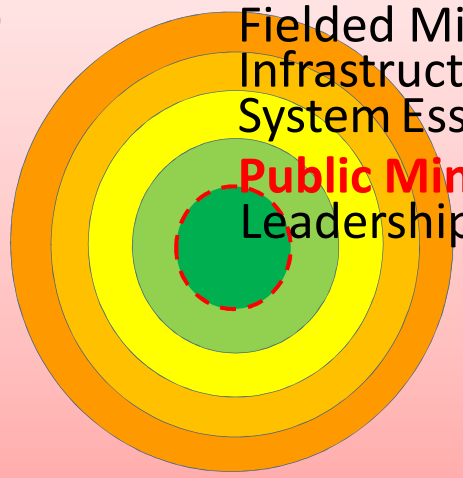
Ⅴ The Implication on Cyber Operation in the Western Pacific and Japan-US Alliance

Clarification of strategic objectives by adapting Cyber 4.5 ring model



Five-Ring Model
（Air Strategy)

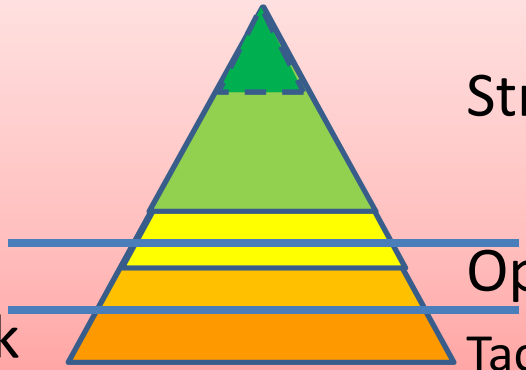
（My Plan）



4.5-Ring Model（Cyber Strategy)

Cyber Decapitation
Cyber Propaganda
（Fake News）
Strategic Cyber Attack

Cyber Espionage
Electromagnetic Attack



Strategic Level

Operational Level

Tactical Level (Mainly EMS)

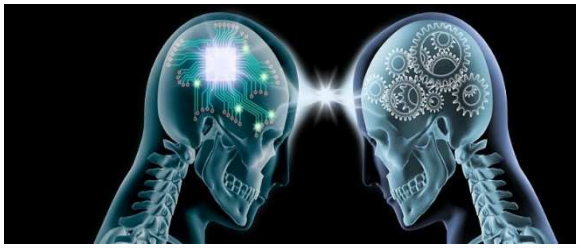
Mind

Physical

It could be a cyber warfare concept against democracies

Ⅴ The Implication on Cyber Operation in the Western Pacific and Japan-US Alliance

Information sharing

learn from small countries



Innovation on Cyber Security